Please describe what would be the best practices for a bank to monitor their infrastructure and business.

As IT infrastructure consists of a variety of inter-related components, a layered approach would be needed, allowing to monitor all components used in the company. Infrastructure may consist of physical servers and devices, cloud providers providing core services, on top of which business-specific applications run. Internal company services interact with each other, but also with ones provided by third parties. Examples of such third-party services may be card issuing, ATMs, integrations with settlement schemes. Some visibility into availability of these is needed as well.

To get an overview of these, it would need a combination of personnel and monitoring technology, which would assist with monitoring the systems. On an organizational level, all the services need to be accounted for and have responsible "owner" teams assigned. This would ensure in case of issues with functionality or performance, issues could be escalated quickly and correctly, investigation started immediately and corrective measures taken.

On a technical side, for all used services central logging and real-time monitoring needs to be in place. Based on that data, it would be necessary to create easily interpretable dashboards, allowing to spot issues when they arise. Dashboards could be implemented in a way that would compare current load to average one, "turning red", when something is beyond acceptable range, service is down or fails with too many errors.

Real-time monitoring of servers, applications, networks, endpoints transactions allows to to see if some unusual patterns emerge, allowing to take action immediately (in case of cyberattacks before adversaries will be able to inflict damage).

Also incident management platforms should be in place - so in case of issues, people would be notified promptly.

—

From a business point of view systems, servers and integrations would need some form of capacity planning - even in the cloud. This is to estimate costs and avoid unexpectedly high charges. While cloud services are typically easily scaleable, misconfigurations, malicious requests or change in usage patterns could mean a very high cloud usage bill at the end of the month. Teams should be assigned a budget for infrastructure expenses and stay strictly within that budget.

Business and IT interaction should be present, it's a good idea to have playbooks in case of IT system failures and incidents. This is both for internal usage - so issues could get addressed and fixed as soon as possible, issues documented properly, understood and prevented from happening again. But also some sort of external communication plan would need to be developed, so that in case of issues, they could be explained simply to external parties.

Externally banks could be affected by impersonation, like malicious messages sent in the name of the bank. So some sort of media/internet monitoring could be in place as well, likely bought in from companies specialized in that.

Regarding more specific issues, disaster recovery plans should be in place and testing of those should be done regularly. For example restoring databases, using backups to recover from disk failures and failovers between active and standby servers. All these should have expected timelines defined and revised if necessary.

It would also make sense to define and track KPIs - key metrics and SLAs, for example number of login sessions, number of transactions, their success/failure rate, average response time for services.

In regards to databases and data warehouses it's important to track data quality, which includes ETL monitoring, data lineage tracking and data quality dashboards.

Banks are all about trust, and there are regulations and cyber security standards in place that describe in detail what aspects should be taken care of.